TECHNIQUES FOR DETECTING COVER AND DECEPTION

Cov'r and Deception [illegible] D)

Robert P. Goldsmith and Ralph F. Gerenz

Betac Corporation
76 Treble Cove Road
Billerica, Massachusetts 01862

Summary

The increasing sophistication of intelligence collection and analysis systems has given US decision makers a powerful tool to evaluate the actions and intentions of our potential adversaries. At the same time, however, these advances have in some respects increased our susceptability to the skillful use of cover and deception techniques. Throughout history, the potential success of ~~C & D~~ operations has been determined soley by the skill of the practitioner, regardless of the sophistication of the intended victim in conducting C & D operations. Today, we face in the Soviet Union a nation which has both recognized the importance of C & D and has over the years demonstrated an impressive capability to deceive and mislead both its intended victims and the US and its allies. This paper outlines the salient characteristics of C & D, Soviet doctrine and application and some of the techniques which could be used to uncover cover and defeat deception.

The Operational Context for Cover and Deception

What is C & D?

"Cover" denies an adversary the intelligence data needed to plan and carry out operations, and it includes both camouflage and avoidance. Camouflage can be either passive, in which case it attempts to make the threatening activity appear either benign or not appear at all, or active, in which threatening activity is simulated where it does not, in fact, exist. Avoidance exploits knowledge of the adversary's collection capabilities and operational use to deny reconnaissance opportunity.

"Deception" seeks to use both camouflage and avoidance, together with genuine but misleading activity, to manage an adversary's perception of events, capabilities and planned actions.

A skillful user of C & D seeks to provide an adversary with pieces of information which appear genuine in themselves, and which fit a course of action which the adversary would find reasonable. In this, the C & D practitioner attempts to exploit the anchoring bias of the cognitive process [1], by presenting the strongest indications of the deception story first. If the intended victim has already formed an estimate of the most likely course of action, the practitioner need only take those actions necessary to provide substantiating evidence. Once the victim has focused on a single most likely course of action, receipt of later information will be evaluated in terms of whether or not it matches the current hypothesis. The victim may then ignore contradictory evidence, fit ambiguous evidence to match the hypothesis as if no ambiguity existed, and accept deceptive activity with little scrutiny.

Cover and Deception and the Intelligence Process

The use of C & D extends across the conflict spectrum, and applies to other dimenrions of military/political analysis. Cover and deception has been successfully applied to manage perceptions during peacetime, crisis and war. Similarly, C & D is a major concern in successful application of arms control and to the maintaining the validity of a deterrence policy. The operational context for C & D is shown in Figure 1.

The opposing decision-maker selects both an operations plan and a C & D plan, the first to acheive his objectives, and the second to manage friendly perceptions in such a way that counter-action will be misdirected or mistimed. These plans are executed as a course of action (1), apects of which can be observed if friendly collection assets are present and active when they occur (2). Threat assessment (3) attempts to correlate information collected with a concept of how opposing forces would be used under a variety of circumstances, to produce an evaluation of what the opposing forces are trying to do. The friendly decision maker then selects a response (4), based on set policy and the capabilities of his own assets.

The principle objective of the intelligence process is knowledge the opposing decision-maker's plan. Usually, this cannot be gained directly. Further, the raw data which the intelligence system receives is limited both by the attributes of military activity which are observable and by the time slices when collectors are actually tasked to collect. Finally, the interpretation of activity depends on the accuracy of our concept of the opponent's force procedures. Even without any intent to deceive by an opponent, the limitations of the intelligence process would leave us with an incomplete and sometimes misleading picture of his activities and objectives.

The threat assessment process is vulnerable to C & D at each step. Figure 2 decomposes the process, and shows the opportunities for a skillful opponent to employ C & D. To begin with, an adversary can control the timing and type of activity by his forces to manage our perception of the observable features of his course of action. Assuming that an analyst began with an accurate baseline of enemy locations and activity, this type of deception would cause errors in threat situation monitoring-monitoring the current state of enemy forces. At this point, the opponent loses direct control over his ability to manage perception, but must rely on the weaknesses of our intelligence analysis system. The opponent's C & D plan attempts to orchestrate observable activity so that collection distortions and interpretation errors are propagated through the higher levels of intelligence analysis.

Indications analysis, relying on an incorrect statement of the current situation, will misdirect requests for additional collection. Key activities will be missed, and others will be assessed as having occurred when they have only been simulated. The final step in the process, threat synthesis, matches key activities with the hypothesized set of courses of actions. If those key activities are not correctly identified, or if the set of courses of action is incomplete, an incorrect assessment of the opposing decision-maker's intentions will be given to our own commanders.

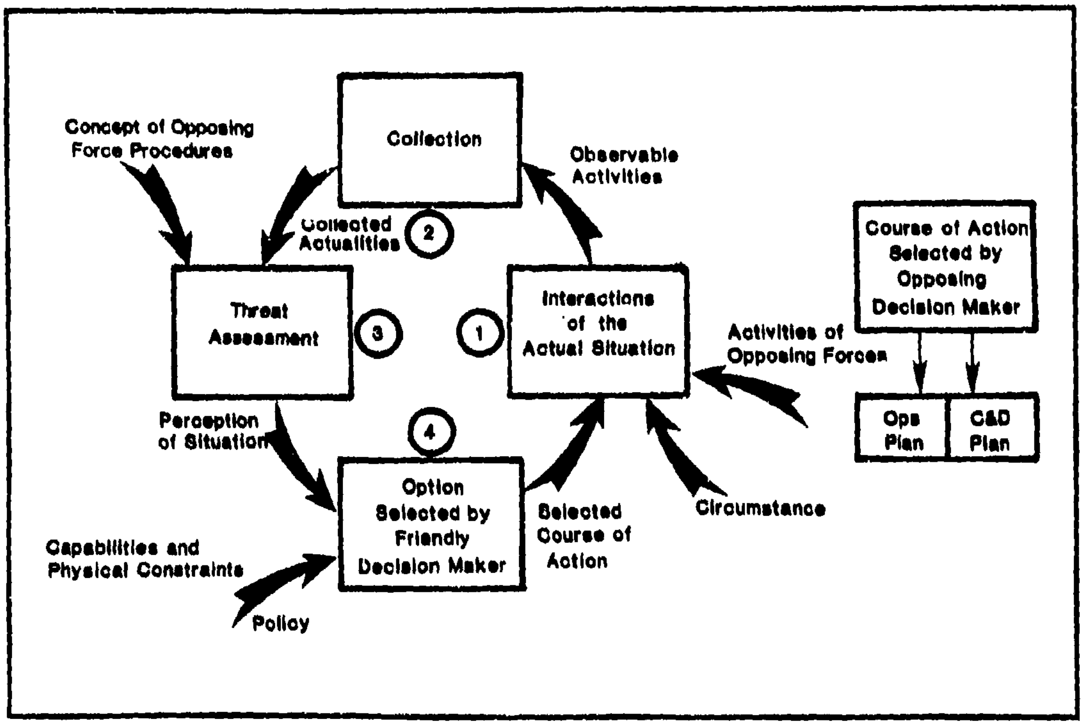
Collection
Concept of Opposing Force Procedures
Observable Activities
Collected Actualities
2
Threat Assessment
3
1
Interactions of the Actual Situation
Course of Action Selected by Opposing Decision Maker
Activities of Opposing Forces
Ops Plan
C&D Plan
Perception of Situation
4
Option Selected by Friendly Decision Maker
Selected Course of Action
Circumstance
Capabilities and Physical Constraints
Policy

FIGURE 1 OPERATIONAL CONTEXT FOR C&D

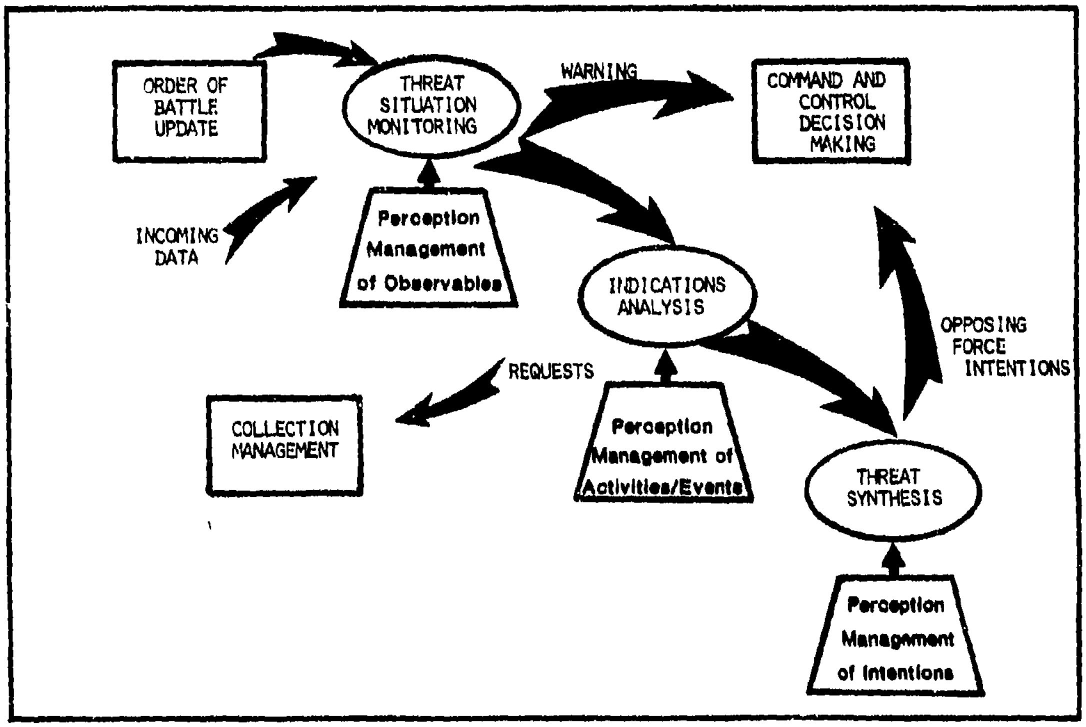
ORDER OF BATTLE UPDATE
THREAT SITUATION MONITORING
WARNING
COMMAND AND CONTROL DECISION MAKING
INCOMING DATA
Perception Management of Observables
INDICATIONS ANALYSIS
OPPOSING FORCE INTENTIONS
REQUESTS
COLLECTION MANAGEMENT
Perception Management of Activities/Events
THREAT SYNTHESIS
Perception Management of Intentions

FIGURE 2 THREAT ASSESSMENT VULNERABILITIES TO C&D

Unfortunately, many of the developments in intelligence systems in recent years have increased our vulnerability to C & D at the same time that they have increased our ability to collect data and to analyze activity. Together with a greatly increased ability to collect, we have developed systems to help the human analyst exploit that capability by focusing attention on items which analysts have identified as keys.[2] Thus, each enemy course of action can be broken down into indicators-steps which must be taken to realize that action, indicators into key activities, activities into observables. The result is a system of great power for focusing attention on significant pieces of information and for leading to conclusions of intent based upon a clear path of reasoning. The weakness of this system is that the discriminators at each step become high value targets for an opponent's C & D activities, and as we discuss in the next section, it is highly likely that the Soviets will attempt to exploit this weakness.

Soviet Cover and Deception Doctrine and Applications

Extensive use of cover and deception techniques in the tactical environment are basic tenets of Soviet military doctrine. Natural Soviet proclivity to secretiveness coupled with Soviet experience and lessons learned over the last thirty years have convinced Soviet leaders that cover and deception are invaluable tools in tactical warfare. These attitudes have undoubtedly been strengthened by the successful application of C&D by both Arabs and Israelis in the Middle East wars, and by the British in the Falklands.

The commonly held Western appreciations of Soviet C&D capabilities may already be out of date. The Soviets have repeatedly demonstrated their ability to make the improvements necessary to bring capability in other fields up to the demands of doctrine. A clear example of this is the comparatively recent development and mass deployment of equipment (such as the KIROV-class VSTOL carrier) which make the extension of Soviet offensive doctrine into the naval domain a credible threat to NATO. A corresponding effort to increase the level and sophistication of their C&D capabilities can therefore be hypothesized as a most likely Soviet course of action.

Soviet Cover and Deception Doctrine

Soviet doctrine for Cover and Deception derives from the doctrinal requirement for surprise, one of the basic principles of what the Soviets call "operational art". These basic principles, in the order assigned by the Soviet author Savkin [3], include:

- Mobility/Tempo
- Concentration of Efforts
- Surprise
- Activeness of Combat
- Preservation of Effectiveness
- Conformity of Goals to Conditions
- Interworking

Mobility/Tempo includes not only speed of movement but also flexibility , such as in changing the axis of an attack. Concentration of efforts is more familiar to us as the principles of mass and economy of force. By "Surprise", the Soviets mean the ability to force an enemy to fight in a situation unfavorable to him- either in a place or time which does not allow him to make full use of his own forces. "Activeness of combat" states the Soviet desire to hold the initiative ; this is also the principle of the offensive. "Preservation of Effectiveness" is the Soviet reaction to the advent of weapons of mass destruction, which require that their forces avoid premature concentration, and that they be equipped to survive in a CBR environment. "Conformity of Goals to Conditions" demands that the commander assign reasonable goals to his forces. Because commanders adhere to this principle, the subordinates can therefore be held accountable for any failure. "Interworking" is the basis for the Soviet combined arms approach to military operations. Interworking refers not only to the coordination leading to joint efforts by combat forces, but also to the coordination of front and reserve units, combat and support units, center and flanks.

One of the significant features of these principles is the degree to which each is often implemented in terms of the others. A surprised enemy, for example, is given no time to recover if the attacking forces maintain the tempo of their attack, and keep the initiative. Also, the dispersion prior to attack necessary to preserve combat effectiveness makes it more difficult for the enemy to determine the time and place of an attack. Finally, the Soviets achieve consistency in their deception plans by a combined arms approach to C&D operations.

In the discussion of methods to achieve surprise, Savkin [4], mentions six general types:

- Lead the enemy astray
- Secrecy of Preparation
- Unexpected Use of Nuclera Weapons
- Deliver attacks at Unexpected place/time
- New means/methods of warfare
- Avoid repetition of methods

The first of these methods, leading the enemy astray with regard to one's intended course of action, is the doctrinal basis for Soviet deception operations, just as secrecy of preparation is the bais for the widespread Soviet use of cover and camouflage for offensive purposes. The last two methods are useful in understanding how the Soviets have been able to continue to surprise their opponents in intervention actions over the past thirty years. In his discussion of "new means and methods of warfare", Savkin explains that this is usually acheived by using existing means in ways unknown to an enemy, rather than by the introduction of a totally new capability. This, together with the avoidance of repetition in the methods of operations, including deception operations, put our intelligence system on notice that hypotheses limited to past patterns of Soviet actions not only fail as aids to detection of new patterns, but also increase the probability that the Soviets will exploit our tendancy to correlate the elements of a new course of action with an old one.

Soviet C&D Experience

A brief summarization of four Soviet C&D operations, beginning with the successful preparations for Operation Bagration in the summer of 1944,[5] illustrates how far the Soviets have progressed in the ability to lead their opponents astray. Knowing the German preoccupation with defending their economic base, in this case the Ukraine, the Soviets covered their preparations for an attack in Belorussia through denying the Germans any information that would contradict that hypothesis. For this reason, the Soviets moved their forces to their jump-off positions under the cover of darkness, and spread the observable indicators of impending attack over the entire eastern front- aerial reconnaissance, bomber sorties and air defense were not concentrated in the central front. Communications activity by units dedicated to the attack was kept to a minimum. Although the Germans expected a summer offensive, Soviet security precautions together with German assessment that the most likely location for an attack was the area which they most feared to lose, combined to leave the Germans unprepared for the Soviet assault. A significant difference between the Soviet C&D operations and the coincident US/British effort to deceive the Germans as to the location of the cross-channel landing, however, was that the deception ended when the attack began. This difference has continued in Soviet operations to this day.

In their preparations for intervention in Czechoslovakia in 1968, the Soviets exploited both Western and Czech preconceptions of the sequence of events which would precede such an action. In 1956, the Soviets had called the Hungarian leaders to Moscow and then invaded. In 1968, the Soviets moved their forces to the military districts bordering Czechoslovakia for a long series of exercises, summoned the Czech leaders to Moscow, and did not invade. Instead, the Czechs were allowed to return hom believing the Soviets would withhold action as long as the Czechs committed no excesses of liberalization. Some Soviet units were recalled from the border areas. Although the Soviets still had sufficient force in place to intervene, both Czechs and the West changed their assessment of Soviet intentions. Both were therefore unprepared when the Soviets, with token elements of other Warsaw Pact nations, invaded in August. It is likely that at least part of the reason for the timing of the invasion was to coincide with the summer vacation season in Europe, when many European decision makers would be on vacation. In addition, the Soviets used a ruse to gain control of the main airfield outside of Prague, sending the landing control party on an Aeroflot flight dressed as tourists. The "tourists" easily overpowered the Czech control tower personnel and then proceeded to handle the landing of the aircraft carrying the leading elements of the invasion force.

The Soviet invasion of Afghanistan [6] is a good illustration of how the Soviets were able to achieve the same end-control of the captial city airfield - while varying the means. This time the Soviets flew in the airfield control party weeks be.ore the invasion as reinforcements for Soviet units already deployed there since September, thus arrousing no curiosity. The Soviets then disarmed the Afghani armored forces by recalling the Afghan ammunition and anti-tank guns for inventory, some of their tanks for winterization and others for the repair of defects. Although western intelligence was not surprised - the US had warned the Soviets twice against intervening in Afghanistan-the Soviet choice of Christmas as the invasion date meant that any Western reaction would be delayed as the leaders hurried back from their vacations. The surprise achieved against the Amin government is reflected by the ease with which Soviet divisions occupied the country.

In its initial stages, the Soviet reaction to the internal political events in Poland were similar to those of 1968. [7] A long series of large-scale military exercises were held in the western military districts, the Polish premier visited Moscow, and no immediate invasion occurred. US and NATO intelligence recognized the clear threat of intervention behind the exercises, and exerted diplomatic pressure upon the Soviets to allow the Poles to settle the party-union conflict. The nature and timing of the coup in December therefore caught both Solidarity and the US and its Allies by surprise. Again the Soviets chose a time (Sunday morning during the Christmas season) when opposing decision makers would be at home, and an unexpected means-the Polish internal security forces. The intended victims of the deception were successfully deceived even though quite sensitive to the possibility of deception. The exercises were widely perceived as a cover for the Soviets' true course of action, but this knowledge did not result in correct assessment of Soviet intentions.

In each of the cases sketched above, a great deal of information indicating the true Soviet courses of action was available. The tactical observables of the Soviet preparations were collected. The capabilities of the forces involved were known as was the general intent. In each case, however, the Soviets succeeded in deceiving their victims as to timing and method. This series of successes makes the development of C&D countering techniques, discussed in the next section, a necessary part of any effort to improve the performance of our own intelligence system.

Developing Techniques to Counter Cover and Deception

Countering deception is a two-step process. The first is to identify the targets for deception, the second is to identify how C&D directed against those targets can be recognized and then exploited. These techniques must then be integrated into both sensor related improvements and into the development of expert systems and other ADP tools for intelligence analysis.

Identifying C&D Vulnerabilities

Identifying C&D vulnerabilities can benefit from the great effort already expended in the development of structured indications and warning systems. These systems break down a range of courses of action into the steps (indicators) required to achieve them, decompose these steps into their key activities, and then identify the observables associated with each key activity. These observables are the high value targets for C&D operations, since by managing an opponent's collection of these observables, the deceiver exerts control on the basis of the victim's perceptions. In order to understand how perceptions can be managed, it is therefore necessary to begin by identifying the sources and methods used to gather intelligence data (see Figure 3). Identifying the targets of C&D involves a "reverse engineering" process (see Figure 4). We know how individual collection sources and disciplines can be exploited by an opponent in a general way, and we know which disciplines are employed to collect given observable. By matching collection means and C&D methods pairs to the association of collection means and observables, we can construct a C&D matrix for each key activity. Figure 5 presents a sample C&D means matrix for one possible key activity-the deployment forward of a technical unit (such as a bridging unit). Large scale deployment of such units would be required prior to the initiation of hostilities. Each row in the matrix summarizes how the observable within a particular collection discipline

COLLECTION DISCIPLINES SENSORS	ACINT	COMINT	ELINT	HUMINT	IRINT	MAGINT	OPTINT	PHOTINT	RADINT	TELINT	VISINT
AIRBORNE		●	●		●	●	●	●		●	●
AIRBORNE DETECTION									●		
AIRBORNE IMAGING									●		
ATTACHE				●							
CASUAL				●							
DEDICATED				●							
FIXED SITE ACTIVE	●										
FIXED SITE PASSIVE	●										
MOBILE ACTIVE	●										
MOBILE PASSIVE	●										
OVERHEAD		●	●		●	●	●	●		●	●
OVERHEAD DETECTION									●		
OVERHEAD IMAGING									●		
SUBSURFACE		●									●
SURFACE			●		●		●	●		●	●
SURFACE FIXED SITE		●							●		
SURFACE MOBILE SITE		●							●		

FIGURE 3 COLLECTION DISCIPLINES AND SENSORS

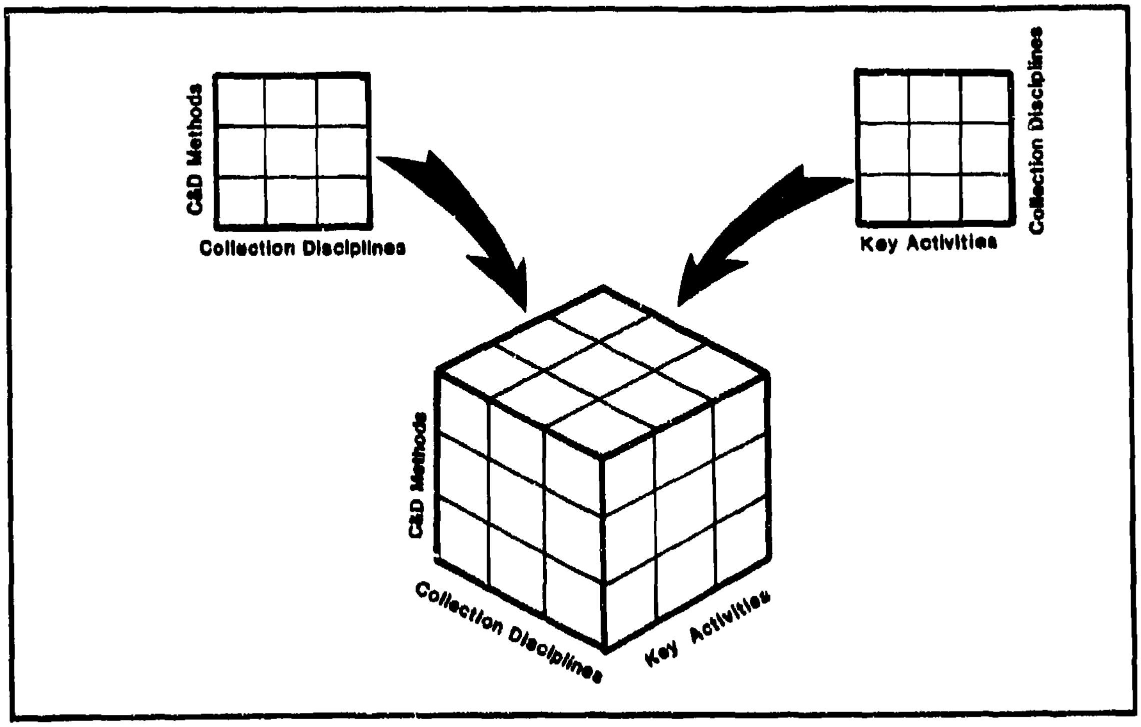

FIGURE 4 DEVELOPING TECHNIQUES TO COUNTER C&D: IDENTIFYING VULNERABILITY

ACTIVITY TO BE CONCEALED OR SIMULATED: DEPLOY TECHNICAL UNIT FORWARD	
COLLECTION DISCIPLINE	COVER & DECEPTION MEANS
ACINT	•SIMULATE SOUND OF VEHICLES
COMINT	•MAINTAIN NORMAL LEVELS OF COMMUNICATIONS AT GARRISON LOCATIONS TO MASK MOVEMENT OF UNITS •MAINTAIN STRICT COMMUNICATIONS SILENCE BY THE MOVING UNITS
ELINT	•STAGGER RADAR CHECK-OUT BEFORE DEPLOYMENT TO SIMULATE NORMAL ACTIVITY •MAINTAIN NORMAL LEVELS AND TYPES OF RADAR ACTIVITY IN GARRISON AREAS
HUMINT	•RELEASE COVERING EXPLANATION FOR ACTIVITY (E.G., EXERCISE ANNOUNCEMENT, TROOP ROTATION)
IRINT	•DEPLOY THROUGH AREAS WITH HIGH LEVELS OF BACKGROUND HEAT (URBAN AREAS, MAJOR ROADS) •DEPLOY THROUGH AREAS WHICH ABSORB IR EMISSIONS •SIMULATE NORMAL GARRISON ACTIVITY WITH NONESSENTIAL VEHICLES
OPINT	•CAMOUFLAGE DEPLOYING VEHICLES AS NON-MILITARY •SIMULATE ESSENTIAL VEHICLES IN GARRISON WITH NONESSENTIAL ONES •MOVE AT NIGHT
PHOTINT	•SIMULATE ESSENTIAL VEHICLES WITH DUMMIES IN GARRISONS
VISINT	•DIVERT FOREIGN OBSERVERS FROM DEPLOYMENT ROUTES •ALLOW OBSERVERS TO SEE STAGED ACTIVITIES ELSEWHERE

FIGURE 5 EXPANSION OF SAMPLE MEANS MATRIX

could be simulated. The more elaborate the deception, the greater number of these methods would be employed, and the larger the number of units simulated.

Uncovering C&D depends upon discovery of inconsistency. The Soviets are likely to apply their military doctrine to C&D operations, in that they will strive to achieve consistency with the least effort necessary (economy of force), and with integration of C&D operations in all domains (interworking). To counter C&D therefore means to progress from line items in the means matrix to correlation of line items in the matrix, and then to the higher levels of the indications structure, as well as to other intelligence disciplines (for example, the order of battle). This search for inconsistency takes place on three levels, each demanding a higher level of man (or machine) intelligence:

- Single collection discipline
- Multiple collection disciplines
- Analytical procedures involving one or more intelligence disciplines

Each technique, properly employed, should stretch the deceiver's web of consistency in the observables harder, until finally it gives way.

Single Discipline Techniques

Single discipline techniques address the weaknesses in the collection and interpretation chain, and can be divided into two types:

- bringing the target into the field of view and
- increasing target discrimination.

Success in either of these can be achieved by improving either the sensor capabilities, the exploitation processing, or even by alerting interpreters to the likelihood of a particular C&D method.

As an example of the application of these techniques, consider an enemy attempting to deploy SAM units forward, and attempting to cover the radar emissions. He may try to keep them out of our ELINT field of view by restricting the time and power of his emissions. They would be brought into the field of view by expanding the duration of coverage, or by deploying more sensitive sensors. This affects both the enemy's ability to avoid coverage, and his ability to remain undetected in the presence of a collector. The enemy might also seek to cover the mass deployment of radars forward by testing them individually, so that the overall level of SAM radar activity in a given area does not change. This can be uncovered by increasing the ability to discriminate among the radar signals of different units with the same types of radars.

Multiple Discipline Techniques

Multiple discipline techniques seek to break down inconsistencies between two or more observables associated with the same key activity. The first step in applying these techniques is to take advantage of the means matrix to identify the opportunities for multiple discipline correlation. There follows a determination of whether the current collection schedules for the sensors involved allow simultaneous coverage. Planning for such coverage increases the burden of activity required to maintain a deception. Finally, the analyst's ability to make effective use of multi-source coverage requires that the interpretation of the collection be organized by activity. For the radar in the above example, therefore, the analyst would be given the PHOTINT, ELINT and other coverage for a particular area over a specified time range. Multiple discipline techniques make cover difficult at the tactical level, and make simulation extremely difficult, since the effort required to simulate an activity in many differnt disciplines may be greater than the effort required by the activity itself.

Analytical Techniques

Beyond current collection and exploitation the intelligence analyst can uncover a C&D operation by comparing current activity with the knowledge base of an opponents capabilities and options. These comparisons are intelligence cross-discipline consistency checks, in which current intelligence is matched with basic intelligence on the one hand and threat assessment on the other.

Basic intelligence provides the analyst with a reference of what an opponent can do. This includes the physical capabilities of equipment-can a mobile radar deploy from A to B in a given time? In addition, it provides an organizational and doctrinal reference for current activity. These are particularly useful in evaluating the activity of the Soviet military, which has minimized organizational variations and which does not encourage deviations from standard operating procedures. A simulated SAM battalion, for example, must include the correct number and relative location of radars, launchers and communications equipment. From the organizational and doctrinal standpoint, it must be co-located with one of a limited number of other types of units. Discrepancies in any of these factors becomes the basis for requests for additional collection, and for expanding the scope of the analytical evaluation.

Once the time and space relationships between indicators and an opponent's likely courses of action have been established, these can also help uncover a C&D operation, and can also help the analyst recognize when the actual course of action does not match any of the hypothesis. One of the major benefits of the structured warning systems is that the analyst can be alerted to the inconsistent absence of activity. This absence could occur under any of the following conditions:

- the activity is present, but is being covered
- the activity not present, and the other key activities are being staged
- the activity is not present, and the other activities are part of a course of action outside the current range of hypotheses

The analyst can identify which explanation applies by increasing collection and exploitation effort to uncover activities if it exists. If it is not found, solutions must be sought along both collection and analysis paths.

In the collection/interpretation domain, increased effort would be applied to determine if some of the observed activities are actually simulations. At the same time, the threat assessment process needs to reevaluate whether the absent activity is a necessary part of a course of action, and whether a new hypothesis would be consistent with the current combination of active and inactive indicators. The discovery of C&D operations during this process has an additional value in that their existance is itself an indication of an opponent's course of action.

Conclusions

Current collection, exploitation and intelligence analysis systems are vulnerable to cover and deception. This vulnerability has increased as analytical aids have tended to focus on the observables associated with the key steps for a limited range of courses of action. Soviet doctrine, with its emphasis on surprise and continuing variations in the means of realizing surprise, is ideally suited to exploit those limitations, and they have been uniformly successful in applying this doctrine to the present day. Both current analysis aids, which are essentially production systems, and the expert systems now under development [8] are basically similar to commercial systems developed for medical, geological or engineering applications. [9] For successful application to military intelligence, the technology must be "hardened" to withstand the skillful use of Cover and Deception.

References

[1] Richards J. Heuer, Jr., "Strategic Deception: A Psychological Perspective," presented at the 21st Annual Convention of the International Studies Association, Los Angeles, California, March 19-22 ,1980.

[2] Ralph F. Gerenz, "A Methodology for Improving the Strategic Warning Process," Journal for Defense Research, Crisis Management Edition, April 1977.

[3] V. Ye. Saukin, The Basic Principles of Operational Art and Tactics (A Soviet View), Moscow, 1972. USAF Translation, Chapter 3, pp. 167-277.

[4] ibid, pp. 230-239.

[5] Barton Whaley, Strategem: Deception and Surprise in War, published in manuscript by M.I.T., Cambridge, Massachusetts, 1969, pp. 144-151.

[6] Jiri Valenti, "Perspectives on Soviet Intervention-Soviet Use of Surprise and Deception," Survival, March/April, 1982, pp. 55-56.

[7] ibid. pp. 57-60.

[8] David Brown and Harvey S. Goodman, "Artificial Intelligence Applied to C3I, "Signal, March, 1983, pp. 27-33.

[9] Avron Barr and Edward Feigenbaum, The Handbook of Artificial Intelligence, Volume 1, pp. 190-199, Los Altos, California: William Kaufman, 1981.